WHAT IS CLAIMED IS:

1.    A method of accessing an electronic file, comprising:

querying a license server associated with an encrypted version of the electronic file in response to a read access request to the electronic file;

issuing a token from said license server according to an access policy when access to the electronic file is authorized; and

decrypting said encrypted version of said electronic file to a volatile memory using said token to produce the electronic file.

2.    The accessing method of claim 1, further comprising:

limiting, after said decrypting step, access by all unauthorized processes to said volatile memory.

3.    The accessing method of claim 1, further comprising:

inhibiting, after said decrypting step, transfer of the electronic file to a nonvolatile memory.

4.    The accessing method of claim 1 wherein said querying step includes extracting a key from said encrypted version of the electronic file and using said key to access said license server.

5.    The accessing method of claim 1 wherein said access policy limits a number of processes that concurrently access the electronic file in said volatile memory.

6.    The accessing method of claim 1 wherein said access policy limits a number of operations on the electronic file in said volatile memory.

7.    The accessing method of claim 1 wherein said access policy selectively enables decryption of a portion of the electronic file.

8.    The accessing method of claim 1 wherein said decrypting step decrypts a portion of the file at any time and overwrites successive portions on top of previously decrypted portions.

9.      The accessing method of claim 1 wherein decrypting step includes both a cryptological function and a tokenization and transformation function.

10.     The accessing method of claim 1 wherein said read request is issued from an access program.

11.     The accessing method of claim 10 wherein said access program is an interpreted program translator and the electronic file is source for said interpreted program translator.

12.     The accessing method of claim 1 wherein said access policy provides for third party access control.

13.     The accessing method of claim 1 wherein said license server is a local file.

14.     The accessing method of claim 1 wherein said license server is a remote file not available on a computing system storing the encrypted electronic file.

15.     The accessing method of claim 1 wherein said license server is coupled to the electronic file.

16.     A method of producing an electronic file having embedded access control, comprising:
        encrypting the electronic file with a first key to produce an encrypted electronic file; and
        associating said encrypted electronic file with an access executable and a license server having an access policy for the electronic file, both operable on a computing system, said license server responsive to an access request from said access executable to issue a first token to said access executable according to said first key and said access policy, and said access executable responsive to said first token to decrypt said encrypted electronic file into a volatile memory protected by said access executable.

17.     The producing method of claim 16 wherein encrypting step includes both a cryptological function and a tokenization and transformation function.

1        18.    A method of providing access to a process executing on a

2  computing system of an encrypted electronic file containing a plain electronic file,

3  comprising:

4        issuing an access instruction from the process to access the plain electronic

5  file;

6        querying a license server associated with the encrypted electronic file in

7  response to said access instruction;

8        issuing a token from said license server according to an access policy

9  when access to the plain electronic file is authorized, said token containing access

10  authorization instructions;

11        decrypting so much of the encrypted electronic file to a volatile memory as

12  authorized by said access authorization instructions to write all or a portion of the plain

13  electronic file into said volatile memory; and

14        providing controlled access of said portion of the plain electronic file in

15  said volatile memory to the process while inhibiting all other accesses to said volatile

16  memory by other processes.

1        19.    A system for accessing an electronic file, comprising:

2        means for querying a license server associated with an encrypted version

3  of the electronic file in response to a read access request to the electronic file;

4        means, coupled to said querying means, for issuing a token from said

5  license server according to an access policy when access to the electronic file is

6  authorized; and

7        means, coupled to said issuing means, for decrypting said encrypted

8  version of said electronic file to a volatile memory using said token to produce the

9  electronic file.

1        20.    A system for producing an electronic file having embedded access

2  control, comprising:

3        means for encrypting the electronic file with a first key to produce an

4  encrypted electronic file; and

5        means, coupled to said encrypting means, for associating said encrypted

6  electronic file with an access executable and a license server having an access policy for

7    the electronic file, both operable on a computing system, said license server responsive to

8    an access request from said access executable to issue a first token to said access

9    executable according to said first key and said access policy, and said access executable

10   responsive to said first token to decrypt said encrypted electronic file into a volatile

11   memory protected by said access executable.

1         21.    A system for providing access to a process executing on a

2    computing system of an encrypted electronic file containing a plain electronic file,

3    comprising:

4         means for issuing an access instruction from the process to access the plain

5    electronic file;

6         means, coupled to said access instruction issuing means, for querying a

7    license server associated with the encrypted electronic file in response to said access

8    instruction;

9         means, coupled to said querying means, for issuing a token from said

10   license server according to an access policy when access to the plain electronic file is

11   authorized, said token containing access authorization instructions;

12        means, coupled to said token issuing means, for decrypting so much of the

13   encrypted electronic file to a volatile memory as authorized by said access authorization

14   instructions to write all or a portion of the plain electronic file into said volatile memory;

15   and

16        means, coupled to said decrypting means, for providing controlled access

17   of said portion of the plain electronic file in said volatile memory to the process while

18   inhibiting all other accesses to said volatile memory by other processes.